100% ENTRAÎNEMENT

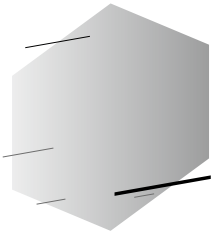
MATHS

MP/MPI

NOUVEAUX PROGRAMMES

Maxime Bailleul
François-Xavier Manoury
Stéphane Préteseille

ellipses



100% ENTRAÎNEMENT

Collection dirigée par Sylvain Rondy

MATHS

MP/MPI

NOUVEAUX PROGRAMMES

Maxime Bailleul
François-Xavier Manoury
Stéphane Préteseille

ellipses

Retrouvez tous les ouvrages de la collection **100% ENTRAÎNEMENT** sur :
www.editions-ellipses.fr



Les macros de cet ouvrage ont été réalisées par Christophe Poulain en LaTeX.

ISBN 9782340-066595
© Ellipses Édition Marketing S.A., 2022
8/10 rue la Quintinie 75015 Paris



Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

www.editions-ellipses.fr

Avant-propos

La collection « 100% entraînement » est conçue pour les élèves des classes préparatoires scientifiques (préparant aux écoles d'ingénieur) et économiques (préparant aux écoles de commerce et de management). L'objectif de cette collection est de mettre l'accent sur l'acquisition d'expérience et d'autonomie, en proposant un grand nombre d'exercices de difficulté progressive, sans rappels de cours excepté dans les corrigés.

Cet ouvrage s'adresse aux élèves des classes préparatoires MP et MPI qui souhaitent trouver un outil différent de celui proposé par les livres d'annales : en effet, chacun des 50 chapitres correspond à une partie du cours bien ciblée et tous les exercices du chapitre portent sur cette partie, ce qui procure un entraînement systématique sur chaque chapitre et permet de s'impliquer réellement dans la maîtrise des notions abordées.

Chaque chapitre est découpé en quatre parties de la façon suivante :

- **Maîtriser le cours.** Cette partie contient « Le Vrai/Faux du début » consistant en des questions de cours ou proches du cours, ainsi que des exercices d'application directe du cours.
- **Maîtriser les méthodes fondamentales.** Cette partie propose des exercices un peu plus compliqués mais proches de méthodes fondamentales qu'il faut absolument connaître et maîtriser parfaitement.
- **Pour aller plus loin.** Cette partie contient des exercices plus élaborés, pour certains difficiles, nécessitant autonomie, faculté à prendre des décisions et esprit de synthèse. Elle se termine par « Le Vrai/Faux de la fin » qui oblige à une réelle réflexion et nécessite d'avoir un bon recul sur les notions abordées.
- **Solution des exercices.** Cette partie fournit les solutions des exercices, complètes et rédigées avec le plus grand soin, au sein desquelles sont disposées des bulles et des encadrés contenant des rappels de cours, des conseils de méthode, des astuces, ou encore des mises en garde contre les erreurs à éviter.

Les auteurs de cette collection ont compilé cet abondant vivier d'exercices afin que ce livre complète efficacement celui de première année.

Sylvain Rondy

Sommaire

Structures algébriques usuelles

1. Groupes et anneaux 1
2. Anneaux $\mathbb{Z}/n\mathbb{Z}$ 11
3. Anneaux $\mathbb{K}[X]$ 20

Réduction des endomorphismes et des matrices carrées

4. Compléments d'algèbre linéaire 26
5. Éléments propres 35
6. Polynôme caractéristique 44
7. Endomorphismes et matrices diagonalisables 52
8. Endomorphismes et matrices trigonalisables 68
9. Endomorphismes nilpotents, matrices nilpotentes 76
10. Polynômes annulateurs et réduction 83

Endomorphismes d'un espace euclidien

11. Adjoint d'un endomorphisme 100
12. Matrices orthogonales 109
13. Isométries vectorielles 116
14. Endomorphismes autoadjoints, matrices symétriques 126

Topologie des espaces vectoriels normés

15. Normes 137
16. Comparaison de normes 150
17. Topologie 161
18. Continuité d'une application 169
19. Compacité 182
20. Connexité 189

Suites et séries de fonctions

21. Compléments sur les séries numériques 194
22. Suites de fonctions : convergence simple et uniforme 212
23. Suites de fonctions : propriétés de la convergence uniforme 224
24. Séries de fonctions : modes de convergence 233
25. Séries de fonctions : propriétés de la convergence uniforme 242

Séries entières

26. Séries entières : rayon de convergence 259
27. Séries entières : propriétés de la somme 269
28. Séries entières : développement 282

Fonctions vectorielles

29. Fonctions vectorielles 291
30. Intégrales impropres 299
31. Intégrabilité 314
32. Intégration par parties, changement de variable 326

Intégration sur un intervalle quelconque

33. Théorème de convergence dominée 340
34. Intégration terme à terme 352
35. Intégrales à paramètres 366

Variables aléatoires discrètes

36. Dénombrabilité 382
37. Espaces probabilisés quelconques 386
38. Variables aléatoires réelles discrètes infinies 401
39. Lois discrètes infinies usuelles 418
40. Couples de variables aléatoires 434
41. Vecteurs aléatoires 455
42. Covariance 473

43. Inégalités probabilistes 484
44. Fonctions génératrices 498

Équations différentielles linéaires

45. Équations différentielles linéaires 514
46. Exponentielle d'une matrice, d'un endomorphisme 526
47. Systèmes différentiels linéaires à coefficients constants 532

Calcul différentiel et optimisation

48. Dérivée suivant un vecteur, dérivée partielle 552
49. Applications différentiables, de classe $\mathscr{C}^1$ et $\mathscr{C}^2$ 558
50. Optimisation 568

1 Groupes et anneaux

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

1. L'ensemble des entiers relatifs pairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
2. L'ensemble des entiers relatifs impairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
3. L'ensemble des multiples de 7 est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☐ Faux

Exercice 2 –

Soit $(G, *)$ un groupe et I un ensemble non vide. Montrer que l'intersection d'une famille $(H_i)_{i\in I}$ de sous-groupes de G est un sous-groupe de G.

Exercice 3 –

Soit $n \in \mathbb{N}^*$ et $\xi = e^{2i\pi/n}$. Montrer que ξ est d'ordre fini dans $(\mathbb{C}^*, \times)$. Quel est le sous-groupe engendré par ξ ?

Exercice 4 –

Le but de cet exercice est de démontrer le théorème de Lagrange dans le cas d'un groupe commutatif : soit $(G, *)$ un groupe commutatif *fini* et x un élément de G. Alors x est d'ordre fini et l'ordre de x divise le cardinal de G.

Fixons x un élément de G.

1. Soit $f : G \to G$ l'application définie par :

$$\forall g \in G, f(g) = g * x$$

   Montrer que f est bijective.

2. Soit n le cardinal de G et $a_1, \dots, a_n$ les éléments de G. Considérons l'élément P de G défini par :

$$P = \prod_{i=1}^{n} a_i$$

   Montrer que :

$$P = P * (x^n)$$

3. En déduire la preuve du théorème de Lagrange.

Exercice 5 –
Soit $\varphi : (A, +_A, \cdot_A) \to (B, +_B, \cdot_B)$ un morphisme d'anneaux commutatifs. Montrer que le noyau de φ est un idéal de $(A, +_A, \cdot_A)$.

Maîtriser les méthodes fondamentales

Exercice 6 –
Soit p, q deux nombres premiers et x, y deux éléments d'ordres p et q d'un groupe abélien $(G, *)$. Montrer que $x * y$ est d'ordre pq.

Exercice 7 –
Soit $(G, *)$ un groupe et e son élément neutre.

1. Soit $x \in G$ tel que $x^{10} = e$ et $x^{21} = e$. Que peut-on dire de x ?
2. Soit $y \in G$ tel que $y^6 = e$ et $y^{22} = e$. Que peut-on dire de y^2 ?

Exercice 8 –
Soit $(\mathbb{K}, +, \cdot)$ un corps. Montrer que les seuls idéaux de ce corps sont $\{0_\mathbb{K}\}$ et $\mathbb{K}$.

Exercice 9 –

Posons $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Z}^2\}$.

1. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ est un anneau (pour les lois usuelles définies sur $\mathbb{R}$).
2. Soit $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{R}$ l'application définie par :

$$\forall (a, b) \in \mathbb{Z}^2,\ N(a + b\sqrt{2}) = a^2 - 2b^2$$

   Montrer que N est bien une application.
3. Montrer que pour tout $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$, $N(xy) = N(x)N(y)$.
4. En déduire les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$.

Exercice 10 –
Soit $(A, +, \cdot)$ un anneau commutatif.
On note 0 son élément neutre pour + et 1 son élément unité pour $\cdot$.
On dit qu'un élément x de A est nilpotent si il existe un entier naturel non nul n tel que $x^n = 0$.
On note $\mathrm{Nil}(A)$ l'ensemble des éléments nilpotents de A. Montrer que $\mathrm{Nil}(A)$ est un idéal de $(A, +, \cdot)$.

Pour aller plus loin

Exercice 11 –
Soit $(G, *)$ un groupe fini de cardinal impair et e son élément neutre.

1. Montrer que $f : G \to G$ définie par $f(g) = g^2$ est une bijection.
2. En déduire que l'équation $g^2 = e$, d'inconnue $g \in G$, admet une unique solution (à savoir e).

Exercice 12 –

Soit $(A, +, \cdot)$ un anneau de Boole, c'est-à-dire un anneau vérifiant la propriété suivante : pour tout $x \in A$, $x^2 = x$.

1. Montrer que, pour tout $x \in A$, $-x = x$.
2. Montrer que A est commutatif.

Exercice 13 – Le vrai/faux de la fin

Soit $n \geq 1$.

1. $\overline{5}$ génère $(\mathbb{Z}/17\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
2. $\overline{5}$ génère $(\mathbb{Z}/15\mathbb{Z}, +)$. ☐ Vrai ☐ Faux
3. $(\mathbb{Z}/8\mathbb{Z}, +)$ contient 4 générateurs. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. L'ensemble des entiers relatifs pairs est un sous-groupe de $(\mathbb{Z}, +)$. ☒ Vrai ☐ Faux
2. L'ensemble des entiers relatifs impairs est un sous-groupe de $(\mathbb{Z}, +)$. ☐ Vrai ☒ Faux
3. L'ensemble des multiples de 7 est un sous-groupe de $(\mathbb{Z}, +)$. ☒ Vrai ☐ Faux

🎓 Cours

On note pour tout entier $n \in \mathbb{N}$:

$$n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$$

Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.

Exercice 2 –

Vérifions les différents points de la caractérisation. Posons :

$$H = \bigcap_{i \in I} H_i$$

- Pour tout $i \in I$, H_i est inclus dans G donc H aussi.
- On note e l'élément neutre de G. Pour tout $i \in I$, $e \in H_i$ car H_i est un sous-groupe de G donc e appartient à H.
- Soit $x, y \in H$. Pour tout $i \in I$, x et y appartiennent à H_i qui est un sous-groupe de G donc $x * y^{-1} \in H_i$. Ainsi,

$$x * y^{-1} \in \bigcap_{i \in I} H_i = H$$

On en déduit que H est un sous-groupe de $(G, *)$.

À retenir

Soit $(G, *)$ un groupe et e son élément neutre.
H est un sous-groupe de $(G, *)$ si et seulement si :

- $H \subset G$.
- $e \in H$.
- $\forall x, y \in H,\ x * y^{-1} \in H$.

Exercice 3 –

On reconnait une racine n-ième de l'unité donc $\xi^n = 1$. De plus, pour tout $k \in \{1, \dots, n-1\}$,

$$0 < \frac{2\pi}{n} \leq 2\frac{k\pi}{n} \leq 2\frac{(n-1)\pi}{n} < 2\pi$$

donc :

$$\xi^k = \mathrm{e}^{2ik\pi/n} \neq 1$$

On en déduit ξ est d'ordre fini égal à n.

Cours

Un élément a d'un groupe $(G, *)$ est d'ordre fini si il existe un entier $k \in \mathbb{N}^*$ tel que a^k soit égal au neutre de G. L'ordre de a est alors le plus petit entier k vérifiant cette propriété.

Déterminons maintenant le sous-groupe engendré par ξ. On a :

$$< \{\xi\} >= \{\xi^k,\ k \in \mathbb{Z}\} = \{\xi^k,\ 0 \leq k \leq n-1\} = \mathbb{U}_n$$

Cours

Soit A une partie d'un groupe $(G, *)$.

- L'intersection de tous les sous-groupes de G contenant A est un sous-groupe de G. C'est le plus petit (au sens de l'inclusion) contenant A. On l'appelle *sous-groupe engendré* par A et on le note $< A >$.
- Si $A = \{x\}$, où $x \in G$, alors :
$$< \{x\} >= \{x^k,\ k \in \mathbb{Z}\}$$

Exercice 4 –

1. Montrons que f est injective. Soit $(g, g') \in G^2$ tel que $f(g) = f(g')$. alors $g * x = g' * x$. On en déduit que :
$$(g * x) * x^{-1} = (g' * x) * x^{-1}$$
donc : Associativité de *
$$g * (x * x^{-1}) = g' * (x * x^{-1})$$
Or $x * x^{-1} = e$ (l'élément neutre de G) donc $g = g'$. Ainsi, f est injective.

Or G est un ensemble fini donc $f : G \to G$ est bijective.

G est fini donc $f : G \to G$ est injective si et seulement si elle est surjective si et seulement si elle est bijective

2. On sait que f est une bijection donc $f(G) = G$ donc $\{a_1, \dots, a_n\} = \{a_1 * x, \dots, a_n * x\}$. Or P est le produit de tous les éléments de G (ce terme a un sens car $*$ est commutative) donc :

$$P = \prod_{i=1}^{n} (a_i * x)$$

Par commutativité de $*$, on en déduit que :

$$P = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} x\right) = P * (x^n)$$

3. D'après la question précédente, on a :

$$P^{-1} * P = P^{-1} * (P * (x^n))$$

Or $*$ est associative et $P^{-1} * P = e$ donc $x^n = e$. On en déduit que x est d'ordre fini et que celui-ci est un diviseur de n, qui est le cardinal de G.

À retenir

Soit a un élément d'ordre fini d d'un groupe $(G, *)$ (dont on note e l'élément neutre). Alors pour tout entier relatif k,

$$a^k = e \iff d | k$$

Exercice 5 –

Cours

On appelle *morphisme* d'un anneau $(A, +_A, \cdot_A)$ dans un anneau $(B, +_B, \cdot_B)$ toute application $\varphi : A \to B$ vérifiant les propriétés suivantes :

- Pour tout $(x, y) \in A^2$, $\varphi(x +_A y) = \varphi(x) +_B \varphi(y)$.
- Pour tout $(x, y) \in A^2$, $\varphi(x \cdot_A y) = \varphi(x) \cdot_B \varphi(y)$.
- $\varphi(1_A) = 1_B$ (où 1_A et 1_B sont les unités des deux anneaux).

L'application φ est un morphisme d'anneaux donc en particulier un morphisme de groupes. Ainsi, $(\mathrm{Ker}(\varphi), +_A)$ est un sous-groupe de $(A, +_A)$.

Soit $a \in A$ et $x \in \mathrm{Ker}(\varphi)$. Alors :

$$\varphi(a \cdot_A x) = \varphi(a) \cdot_B \varphi(x) = \varphi(a) \cdot_B 0_B = 0_B$$

donc $a \cdot_A x \in \mathrm{Ker}(\varphi)$.

Ainsi, le noyau de φ est un idéal de $(A, +, \cdot)$.

Cours

Soit $(A, +, \cdot)$ un anneau commutatif et I une partie de A. On dit que I est un *idéal* de $(A, +, \cdot)$ si :

- $(I, +)$ est un sous-groupe de $(A, +)$.
- Pour tout $a \in A$ et tout $x \in I$, $a \cdot x \in I$.

Exercice 6 –

Notons e l'élément neutre de $(G, *)$. Par commutativité de $*$, on a :

$$(x * y)^{pq} = (x^p)^q * (y^q)^p = (e^q) * (e^p) = e$$

donc $x * y$ est d'ordre fini et son ordre divise pq. Soit $r \in \mathbb{N}^*$ tel que $(x * y)^r = e$. On a donc $(x^r) * (y^r) = e$ et en multipliant par y^{-1}, r fois à droite, on a :

$$x^r = (y^{-1})^r$$

puis :

$$x^{pr} = (y^{-1})^{pr}$$

Or $x^p = e$ donc $x^{pr} = e$ ce qui implique que $(y^{-1})^{pr} = e$. On en déduit que $y^{pr} = e$ donc q divise pr par propriété de l'ordre d'un élément.
Or p et q sont premiers entre eux donc q divise r. Lemme de Gauss
De même, on prouve que p divise r. Or p et q sont premiers entre eux donc pq divise r.

On en déduit que pq est l'ordre de xy.

Exercice 7 –

1. Par hypothèse x est d'ordre fini et en notant n son ordre, on sait que n divise 10 et n divise 21. Or le PGCD de 10 et 21 est 1. On en déduit que n divise 1 donc $n = 1$. Ainsi, $x^1 = e$ donc $x = e$.
2. Par hypothèse y est d'ordre fini et en notant m son ordre, on sait que m divise 6 et 22. Or le PGCD de 6 et 22 vaut 2. On en déduit que m divise 2 donc $m = 1$ ou $m = 2$.
   - Si $m = 1$ alors $y = e$ donc $y^2 = e$.
   - Si $m = 2$ alors $y^2 = e$.

   Ainsi, dans tous les cas, $y^2 = e$.

Exercice 8 –

Soit I un idéal de $(\mathbb{K}, +, \cdot)$. Si I est différent de $\{0_{\mathbb{K}}\}$, il contient au moins un élément y non nul de $\mathbb{K}$. Par définition d'un corps, on sait que y est inversible et $y^{-1} \in \mathbb{K}$. Par définition d'un idéal, en notant 1 l'élément unité du corps, on en déduit que $1 = y^{-1} \cdot y \in I$. De nouveau par définition d'un idéal, on a :

$$\forall x \in \mathbb{K}, x = x \cdot 1 \in I$$

Ainsi, $I = \mathbb{K}$.

Exercice 9 –

1. Il suffit de montrer que c'est un sous anneau de $(\mathbb{R}, +, \cdot)$.

- $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$.
- Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. Il existe des entiers relatifs a, b, c et d tels que :

$$x = a + b\sqrt{2} \text{ et } y = c + d\sqrt{2}$$

Par simple calcul, on a :

$$x - y = (a - c) + (b - d)\sqrt{2} \text{ et } xy = ac + 2bd + (bc + ad)\sqrt{2}$$

Or $a-c, b-d, ac+2bd$ et $bc+ad$ sont des entiers relatifs donc $x-y$ et xy appartiennent à $\mathbb{Z}[\sqrt{2}]$.

- On a $1 = 1 + 0\sqrt{2}$ et $(1, 0) \in \mathbb{Z}^2$ donc $1 \in \mathbb{Z}[\sqrt{2}]$.

Ainsi, $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $(\mathbb{R}, +, \cdot)$.

Cours

Soit $(A, +, \cdot)$ un anneau (et 1_A son élément unité) et B une partie de A. Alors B est un sous-anneau de A si et seulement si :

$$\begin{cases} \forall (x, y) \in B^2,\ x - y \in B \text{ et } x \cdot y \in B \\ 1_A \in B \end{cases}$$

2. Soit a, b, c et d des entiers relatifs. Supposons que :

$$a + b\sqrt{2} = c + d\sqrt{2}$$

On en déduit que :

$$a - c = (d - b)\sqrt{2}$$

Sachant que $\sqrt{2}$ est irrationnel, et que $a - c$ et $d - b$ sont des entiers relatifs, on a $d = b$ et $a = c$. Finalement :

$$N(a + b\sqrt{2}) = N(c + d\sqrt{2})$$

L'application N est donc bien définie.

À retenir

Soit E et F deux ensembles. Une application $f : E \to F$ est bien définie si :

$$\forall x \in E,\ \exists! y \in F,\ f(x) = y$$

3. Soit $x, y \in \mathbb{Z}[\sqrt{2}]$. Il existe des entiers relatifs a, b, c et d tels que :

$$x = a + b\sqrt{2} \text{ et } y = c + d\sqrt{2}$$

On a déjà montré que :

$$xy = ac + 2bd + (bc + ad)\sqrt{2}$$

donc :

$$\begin{aligned} N(xy) &= (ac+2bd)^2 - 2(bc+ad)^2 \\ &= a^2c^2 + 4acbd + 4b^2d^2 - 2b^2c^2 - 4bcad - 2a^2d^2 \\ &= a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2 \end{aligned}$$

Or on a :

$$\begin{aligned} N(x)N(y) &= (a^2-2b^2)(c^2-2d^2) \\ &= a^2c^2 - 2a^2d^2 - 2b^2c^2 + 4b^2d^2 \end{aligned}$$

ce qui donne l'égalité souhaitée.

4. Raisonnons par analyse-synthèse.

Analyse. Soit $x \in \mathbb{Z}[\sqrt{2}]$ inversible. Alors il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. D'après la question précédente, on a donc :

$$N(x)N(y) = N(1) = 1$$

Or N est à valeurs dans $\mathbb{Z}$ donc $N(x) = \pm 1$.

Synthèse. Réciproquement, soit $x \in \mathbb{Z}[\sqrt{2}]$ tel que $N(x) = \pm 1$. Il existe $(a,b) \in \mathbb{Z}^2$ tel que :

$$x = a + b\sqrt{2}$$

et par hypothèse, $a^2 - 2b^2 = \pm 1$ donc $x \neq 0$ (si x est nul, $a = b = 0$ car $\sqrt{2}$ est irrationnel). On a alors :

$$\frac{1}{x} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \pm(a-b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$$

Ainsi, x est inversible dans $\mathbb{Z}[\sqrt{2}]$.

Les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont donc les éléments de la forme $a + b\sqrt{2}$ où $(a,b) \in \mathbb{Z}^2$ et $a^2 - 2b^2 = \pm 1$.

Exercice 10 –

Vérifions les différents points de la caractérisation.

- $\mathrm{Nil}(A) \subset A$.
- 0 appartient à $\mathrm{Nil}(A)$ car $0^1 = 0$.
- Soit $x, y \in \mathrm{Nil}(A)$. Il existe deux entiers naturels non nuls n et m tels que $x^n = 0$ et $y^m = 0$. Pour tout entier $p \geq 1$, on a :

L'anneau est commutatif

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \cdot y^{p-k}$$

Si chaque terme de la somme est nul, alors $x + y$ est nilpotent.

Or pour tout entier naturel k, si $k \geq n$ alors $x^k = 0$. Ainsi, si $p \geq n$:

$$(x+y)^p = \sum_{k=0}^{n-1} \binom{p}{k} x^k \cdot y^{p-k}$$

De même, pour tout entier naturel k, si $p - k \geq m$ (ce qui est équivalent à $k \leq p - m$) alors $y^{p-k} = 0$. On en déduit que :

$$(x+y)^p = \sum_{k=p-m+1}^{n-1} \binom{p}{k} x^k \cdot y^{p-k}$$

Si $p - m + 1 > n - 1$ alors la somme précédente est vide donc $(x+y)^p = 0$. Il suffit de choisir $p = m + n - 1 \in \mathbb{N}^*$. Ainsi, $x + y \in \mathrm{Nil}(A)$.

Cours – Binôme de Newton.

Soit $(A, +, \cdot)$ un anneau et $(a, b) \in A^2$. Si $a \cdot b = b \cdot a$ alors pour tout entier $n \geq 0$:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$$

- Soit $x \in \mathrm{Nil}(A)$ et $a \in A$. Il existe un entier naturel non nul n tel que $x^n = 0$. Alors :

$$(a \cdot x)^n = a^n \cdot x^n = a^n \cdot 0 = 0$$

  On en déduit que $a \cdot x \in \mathrm{Nil}(A)$.
- Pour tout $x \in \mathrm{Nil}(A)$, $-x \in \mathrm{Nil}(A)$ (car $-x = -1 \times x$).

Ainsi, $\mathrm{Nil}(A)$ est un idéal de $(A, +, \cdot)$.

Exercice 11 –

1. L'ensemble G est fini donc il suffit de montrer que f est surjective. Le cardinal de G est impair donc il existe un entier naturel m tel que $\mathrm{Card}(G) = 2m + 1$. Pour tout élément x de G, on a d'après le théorème de Lagrange :

$$(x^{m+1})^2 = x^{2m+2} = x^{2m+1} * x = x$$

   car l'ordre d'un élément divise le cardinal du groupe. Ainsi :

$$x = f(x^{m+1})$$

   On en déduit que f est surjective donc bijective.
2. L'élément e admet un unique antécédent par f, ce qui donne le résultat.

Exercice 12 –

1. Soit $x \in A$. On a :

$$(x+x)^2 = x + x$$

ce qui donne en développant :

x commute avec x

$$x^2 + 2 \cdot x^2 + x^2 = 2 \cdot x$$

donc $x + 2 \cdot x + x = 2 \cdot x$ ou encore $x + x = 0$ ce qui implique que $x = -x$.

2. Soit $x, y \in A$. On sait que :

$$(x + y)^2 = x + y$$

donc

$$x^2 + x \cdot y + y \cdot x + y^2 = x + y$$

donc

$$x + x \cdot y + y \cdot x + y = x + y$$

donc $x \cdot y = -y \cdot x = y \cdot x$ d'après la question précédente.

Exercice 13 –

1. Vrai. Pour tout entier relatif k, $\overline{k}$ génère $(\mathbb{Z}/17\mathbb{Z}, +)$ si et seulement si k et 17 sont premiers entre eux.

2. Faux. Le PGCD de 5 et 15 vaut 5.

3. Vrai. Ce sont $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$.

À retenir

Soit $n \in \mathbb{N}^*$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences de $\mathbb{Z}$ pour la relation de congruence modulo n. On a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

et cet ensemble a n éléments.

La relation de congruence modulo n est compatible avec l'addition :

$$\forall (x, x', y, y') \in \mathbb{Z}^4,\ (x \equiv x'\ [n] \ \text{ et } \ y \equiv y'\ [n]) \implies x + y \equiv x' + y'\ [n]$$

Cela permet de définir la somme de deux éléments de $\mathbb{Z}/n\mathbb{Z}$. Soit $(\alpha, \beta) \in (\mathbb{Z}/n\mathbb{Z})^2$. Il existe deux entiers x et y tels que $\alpha = \overline{x}$ et $\beta = \overline{y}$. On pose alors :

$$\alpha + \beta = \overline{x + y}$$

Cette définition a bien un sens car si x' et y' sont deux entiers tels que $\alpha = \overline{x'}$ et $\beta = \overline{y'}$ alors d'après la compatibilité avec l'addition :

$$\overline{x + y} = \overline{x' + y'}$$

Ainsi, la définition de la somme ne dépend donc pas des représentants de α et β. Il est alors facile de montrer que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

2 Anneaux $\mathbb{Z}/n\mathbb{Z}$

Dans la suite, $\overline{x}$ désigne la classe d'équivalence d'un entier relatif x dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$ considéré dans l'exercice.

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

1. $\overline{2}$ est inversible dans $\mathbb{Z}/15\mathbb{Z}$. ☐ Vrai ☐ Faux

2. $\overline{3}$ est inversible dans $\mathbb{Z}/18\mathbb{Z}$. ☐ Vrai ☐ Faux

3. $(\mathbb{Z}/13\mathbb{Z}, +, \cdot)$ est un corps. ☐ Vrai ☐ Faux

Exercice 2 –

Déterminer, avec peu de calculs, l'ensemble des solutions du système de congruences suivant :

$$(S) \begin{cases} k & \equiv & 1\ [3] \\ k & \equiv & 2\ [5] \end{cases}$$

Exercice 3 –

Soit φ la fonction indicatrice d'Euler. Déterminer :

1. $\varphi(13)$.

2. $\varphi(16)$.

3. $\varphi(600)$.

4. Le nombre d'éléments inversibles dans $(\mathbb{Z}/56\mathbb{Z}, +, \cdot)$.

Exercice 4 –

En utilisant le théorème d'Euler, déterminer le reste de la division euclidienne de 13^{178} par 15.

Maîtriser les méthodes fondamentales

Exercice 5 –

Résoudre le système de congruences suivant :

$$\begin{cases} x & \equiv & 4\ [22] \\ x & \equiv & 2\ [13] \end{cases}$$

Exercice 6 –

1. Déterminer l'inverse de $\overline{3}$ dans $\mathbb{Z}/4\mathbb{Z}$, après avoir justifié son existence.
2. Faire de même avec $\overline{17}$ dans $\mathbb{Z}/31\mathbb{Z}$.

Exercice 7 –

Résoudre $x^2 = \overline{1}$ dans $\mathbb{Z}/8\mathbb{Z}$.

Exercice 8 –

Résoudre $5x = \overline{2}$ dans $\mathbb{Z}/34\mathbb{Z}$.

Pour aller plus loin

Exercice 9 –

Soit n un entier naturel supérieur ou égal à 2. On souhaite montrer le résultat suivant : n est premier si et seulement si $(n-1)! \equiv -1\ [n]$.

1. Supposons n premier.
   a) Déterminer les solutions de $x^2 = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$.
   b) Montrer que $(n-1)! \equiv -1\ [n]$.
2. On suppose que $(n-1)! \equiv -1\ [n]$. Montrer que pour tout $a \in [\![1\,;\ n-1]\!]$, $a \wedge n = 1$. En déduire le résultat souhaité.

Exercice 10 –

Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un entier pair.

Exercice 11 –

Soit $n \in \mathbb{N}^*$.

1. Caractériser et dénombrer les inversibles de l'anneau $\mathbb{Z}/2^n\mathbb{Z}$.
2. Soit $x \in \mathbb{Z}$ tel que $\overline{x}$ soit inversible dans $\mathbb{Z}/2^n\mathbb{Z}$. Donner deux algorithmes du calcul de l'inverse de x modulo 2^n :
   - le premier utilisant la suite $(\overline{x}^{2^k})_{k\geq 0}$;
   - le second résolvant successivement, pour $k = 1, \dots, n$, l'équation $y_k x \equiv 1\ [2^k]$ d'inconnue y_k.

Exercice 12 – Le vrai/faux de la fin

Soit $n \in \mathbb{N}^*$.

1. Un polynôme à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ a au plus n racines. ☐ Vrai ☐ Faux
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est intègre. ☐ Vrai ☐ Faux
3. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ a un nombre pair d'inversibles. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. $\overline{2}$ est inversible dans $\mathbb{Z}/15\mathbb{Z}$.	☒ Vrai	☐ Faux
2. $\overline{3}$ est inversible dans $\mathbb{Z}/18\mathbb{Z}$.	☐ Vrai	☒ Faux
3. $(\mathbb{Z}/13\mathbb{Z}, +, \cdot)$ est un corps.	☒ Vrai	☐ Faux

🎓 Cours

Soit $n \in \mathbb{N}^*$.

- Pour tout entier relatif k, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k \wedge n = 1$.
- On en déduit que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier. Ce corps est alors noté $\mathbb{F}_n$.

Exercice 2 –

Les entiers 3 et 5 sont premiers entre eux. D'après le théorème chinois, le système (S) admet une unique solution modulo $3 \times 5 = 15$. Il suffit donc de trouver une solution particulière.

En testant des petites valeurs, on remarque que 7 est solution de (S). On en déduit que l'ensemble des solutions de (S) est :

$$\{7 + 15k,\ k \in \mathbb{Z}\}$$

🎓 Cours – Théorème chinois.

Soit n et m deux entiers naturels non nuls et premiers entre eux. Alors l'application :

$$\begin{array}{rccc} \Phi & : & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & & \overline{x}_{nm} & \mapsto & (\overline{x}_n, \overline{x}_m) \end{array}$$

est un isomorphisme d'anneaux.

Par définition d'une bijection, pour tout $(a, b) \in \mathbb{Z}^2$, il existe donc un entier relatif $k \in \mathbb{Z}$ tel que :

$$\begin{cases} k & \equiv & a\ [n] \\ k & \equiv & b\ [m] \end{cases}$$

Cet entier est unique modulo nm. Autrement dit, un entier relatif ℓ est solution du système précédent si et seulement si $\ell \equiv k\ [nm]$.

Exercice 3 –

1. L'entier 13 est premier donc $\varphi(13) = 12$.

Si p est un nombre premier, $\varphi(p) = p - 1$

Cours

La *fonction indicatrice d'Euler* est l'application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ qui à tout entier $n > 0$, associe le nombre d'entiers $k \in [\![1\,;\, n-1]\!]$ premiers avec n.

2. On a $16 = 2^4$ et 2 est premier donc :

$$\varphi(16) = 2^4 - 2^3 = 8$$

À retenir

Soit p un nombre premier. Pour tout entier naturel $k \geq 1$:

$$\varphi(p^k) = p^k - p^{k-1}$$

3. On décompose 600 en produit de nombres premiers :

$$600 = 6 \times 100 = 2 \times 3 \times 4 \times 25 = 2^3 \times 3 \times 5^2$$

Les entiers 2, 3 et 5 sont premiers donc :

$$\begin{aligned}\varphi(600) &= \varphi(2^3)\,\varphi(3)\,\varphi(5^2)\\ &= (2^3 - 2^2) \times 2 \times (5^2 - 5)\\ &= 4 \times 2 \times 20\\ &= 160\end{aligned}$$

À retenir

Soit n et m deux entiers naturels non nuls premiers entre eux. Alors $\varphi(nm) = \varphi(n)\varphi(m)$.

4. Il suffit de calculer $\varphi(56)$. On a :

$$56 = 8 \times 7 = 2^3 \times 7$$

Les entiers 2 et 7 sont premiers donc :

$$\varphi(56) = \varphi(2^3)\,\varphi(7) = (2^3 - 2^2) \times 6 = 24$$

Ainsi, il y a 24 éléments inversibles dans $(\mathbb{Z}/56\mathbb{Z}, +, \cdot)$.

Cours

Pour tout entier $n \geq 1$, $\varphi(n)$ est :

- Le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
- Le nombre d'inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.

Exercice 4 –

Sachant que $15 = 3 \times 5$, et que 3 et 5 sont premiers, on a :

$$\varphi(15) = \varphi(3)\,\varphi(5) = 2 \times 4 = 8$$

Or 13 et 15 sont premiers entre eux donc d'après le théorème d'Euler :

$$13^{\varphi(15)} \equiv 1\ [15]$$

donc :

$$13^8 \equiv 1\ [15]$$

Remarquons que $178 = 8 \times 22 + 2$. On écrit alors :

$$(13^8)^{22} \equiv 1^{22}\ [15]$$

donc :

$$13^{176} \equiv 1\ [15]$$

et ainsi :

$$13^{178} \equiv 13^2\ [15]$$

Or $13 = 15 - 2$ donc :

$$13^{178} \equiv (-2)^2\ [15]$$

et finalement, $13^{178} \equiv 4\ [15]$. Or $4 \in \{0, \dots, 14\}$ donc 4 est le reste de la division euclidienne de 13^{178} par 15.

Cours – Théorème d'Euler.

Soit $n \geq 1$. Pour tout entier $x \in \mathbb{Z}$ tel que $\overline{x}$ soit inversible dans $\mathbb{Z}/n\mathbb{Z}$, on a :

$$\overline{x}^{\varphi(n)} = \overline{1}$$

ce qui se réécrit :

$$x^{\varphi(n)} \equiv 1\ [n]$$

Exercice 5 –

Les entiers 22 et 13 sont premiers entre eux donc d'après le théorème chinois, ce système admet une unique solution modulo $22 \times 13 = 286$.

Pour déterminer une solution particulière, on cherche une relation de Bézout. On utilise l'algorithme d'Euclide :

$$\begin{aligned} 22 &= 1 \times 13 + 9 \\ 13 &= 1 \times 9 + 4 \\ 9 &= 2 \times 4 + 1 \end{aligned}$$

Ainsi :

$$1 = 9 - 2 \times 4$$

puis :

$$1 = 9 - 2 \times (13 - 9) = 3 \times 9 - 2 \times 13$$

et finalement :

$$1 = 3 \times (22 - 13) - 2 \times 13 = 3 \times 22 - 5 \times 13$$

Posons alors $k_1 = 3 \times 22$ et $k_2 = -5 \times 13$. Alors :

$$k_1 \equiv 0\ [22] \quad \text{et} \quad k_1 \equiv 1\ [13]$$

et :

$$k_2 \equiv 1\ [22] \quad \text{et} \quad k_2 \equiv 0\ [13]$$

On pose alors :

$$x = 2 \times k_1 + 4 \times k_2 = -128$$

D'après les congruences obtenues, on en déduit que x est solution du système. Ainsi, l'ensemble des solutions du système est :

$$S = \{-128 + 286k,\ k \in \mathbb{Z}\} = \{158 + 286k,\ k \in \mathbb{Z}\}$$

Méthode

Soit n et m deux entiers naturels non nuls premiers entre eux. On considère un système de congruences de la forme :

$$\begin{cases} k & \equiv & a\ [n] \\ k & \equiv & b\ [m] \end{cases}$$

où $(a, b) \in \mathbb{Z}^2$. Pour déterminer une solution particulière, on peut tester des petites valeurs (si n et m sont « petits ») ou suivre la démarche suivante :

- On détermine une relation de Bézout : $nu + mv = 1$ où $(u, v) \in \mathbb{Z}^2$.
- On pose $k_1 = nu$. Alors $k_1 \equiv 0\ [n]$ et $k_1 \equiv 1\ [m]$.
- On pose $k_2 = mv$. Alors $k_2 \equiv 1\ [n]$ et $k_2 \equiv 0\ [m]$.
- L'entier $bk_1 + ak_2$ est alors solution du système.
- Toutes les solutions sont alors données par le théorème chinois.

Exercice 6 –

Cours

Soit $n \geq 1$. La classe $\overline{r}$ d'un entier relatif r est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si r et n sont premiers entre eux.

1. Les entiers 3 et 4 sont premiers entre eux donc $\overline{3}$ est inversible dans $\mathbb{Z}/4\mathbb{Z}$. Il est facile de remarquer que $\overline{3} \times \overline{3} = \overline{9} = \overline{1}$. Ainsi, l'inverse de $\overline{3}$ dans $\mathbb{Z}/4\mathbb{Z}$ (qui est commutatif) est lui-même.
2. Les entiers 17 et 31 sont premiers entre eux donc $\overline{17}$ est inversible dans $\mathbb{Z}/31\mathbb{Z}$. Déterminons une relation de Bézout liée à 17 et 31.

$$\begin{aligned} 31 &= 1 \times 17 + 14 \\ 17 &= 1 \times 14 + 3 \\ 14 &= 4 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \end{aligned}$$

On remonte alors les calculs :

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (14 - 4 \times 3) \\ &= 5 \times 3 - 14 \\ &= 5 \times (17 - 14) - 14 \\ &= 5 \times 17 - 6 \times 14 \\ &= 5 \times 17 - 6(31 - 17) \\ &= 11 \times 17 - 6 \times 31 \end{aligned}$$

On en déduit que dans $\mathbb{Z}/31\mathbb{Z}$, $\overline{1} = \overline{11} \times \overline{17}$ donc $\overline{11}$ est l'inverse de $\overline{17}$ dans $\mathbb{Z}/31\mathbb{Z}$.

Méthode

Pour trouver l'inverse d'un élément de $\mathbb{Z}/n\mathbb{Z}$, on dispose de deux méthodes simples :

- Si n est « petit », on calcule les multiples de l'élément considéré.
- Si n est « grand », on trouve une relation de Bézout.

Exercice 7 –

L'ensemble $\mathbb{Z}/8\mathbb{Z}$ contient uniquement 8 éléments $(\overline{0}, \dots, \overline{7})$. Il suffit de tester toutes les possibilités. On remarque alors que $\overline{1}^2 = \overline{1}$, $\overline{3}^2 = \overline{9} = \overline{1}$, $\overline{5}^2 = \overline{25} = \overline{1}$ et $\overline{7}^2 = (\overline{-1})^2 = \overline{1}$. L'équation proposée a donc 4 solutions qui sont $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$.

À retenir

Pour résoudre une équation dans $\mathbb{Z}/n\mathbb{Z}$ avec n « petit », il suffit de tester toutes les valeurs possibles pour obtenir les solutions.
Dans le cas précédent, il est inutile de tester les classes d'entiers pairs car celles-ci ne sont pas inversibles dans $\mathbb{Z}/8\mathbb{Z}$.

Exercice 8 –

Les entiers 5 et 34 sont premiers entre eux. On en déduit que $\overline{5}$ est inversible dans $\mathbb{Z}/34\mathbb{Z}$. Remarquons que :

$$\overline{5} \times \overline{7} = \overline{35} = \overline{1}$$

Ainsi, par multiplication par un élément inversible, on a pour $x \in \mathbb{Z}/34\mathbb{Z}$:

$$5x = \overline{2} \iff 35x = \overline{14} \iff x = \overline{14}$$

L'unique solution de l'équation est donc $\overline{14}$.

Exercice 9 –

1. **a)** On sait que n est premier donc $\mathbb{Z}/n\mathbb{Z}$ est un corps donc intègre. On en déduit que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$:

$$x^2 = \overline{1} \iff (x-\overline{1})(x+\overline{1}) = \overline{0} \iff x = \pm\overline{1}$$

Ainsi, $\overline{1}$ et $\overline{-1}$ sont les deux solutions de l'équation (sauf si $n = 2$ car dans ce cas, $\overline{1} = \overline{-1}$).

b) On a :

$$\overline{(n-1)!} = \overline{1} \times \overline{2} \times \cdots \times \overline{n-2} \times \overline{n-1}$$

Dans ce produit, chaque élément $\overline{k}$ est multiplié par son inverse (rappelons que $\mathbb{Z}/n\mathbb{Z}$ est un corps) sauf $\overline{1}$ et $\overline{n-1} = \overline{-1}$ (si $n > 2$) d'après la question précédente. Ainsi pour $n > 2$:

$$\overline{(n-1)!} = \overline{1} \times \overline{-1} = \overline{-1}$$

et on obtient $\overline{1} = \overline{-1}$ dans le cas où $n = 2$. Ainsi, dans tous les cas :

$$(n-1)! \equiv -1\ [n]$$

2. Par hypothèse, il existe un entier relatif k tel que $(n-1)! - nk = -1$. Si $a \in [\![1\,;\, n-1]\!]$, alors a divise $(n-1)!$ donc il existe un entier p tel que $(n-1)! = pa$. Ainsi :

$$pa - nk = -1 \text{ donc } nk - pa = 1$$

D'après le théorème de Bézout, on en déduit que a et n sont premiers entre eux. Ceci est vrai pour tout $a \in [\![1\,;\, n-1]\!]$ donc n est premier.

Exercice 10 –

Soit $n \geq 3$. Si n admet un diviseur premier impair p, il existe un entier $k \geq 1$ et un entier j premier avec p tel que :

$$n = p^k j$$

On a :

$$\varphi(n) = \varphi(p^k)\varphi(j) = (p^k - p^{k-1})\varphi(j) = p^{k-1}(p-1)\varphi(j)$$

et $p - 1$ est pair. Ainsi, $\varphi(n)$ est pair.

Si n n'admet aucun diviseur premier impair, il existe un entier $k \geq 2$ tel que $n = 2^k$ ($n \geq 3$) donc :

$$\varphi(n) = 2^k - 2^{k-1} = 2^{k-1}$$

donc $\varphi(n)$ est pair.

Exercice 11 –

1. Soit $k \in \mathbb{Z}$. Alors $\overline{k}$ est inversible dans $\mathbb{Z}/2^n\mathbb{Z}$ si et seulement si k et 2^n sont premiers entre eux ce qui est équivalent au fait que 2 ne divise pas k. Le nombre d'inversibles dans $\mathbb{Z}/2^n\mathbb{Z}$ est égal à :

$$\varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$$

2. Suivons la première méthode proposée. D'après le théorème d'Euler, on sait que :

$$\overline{x}^{\varphi(2^n)} = \overline{1}$$

donc :

$$\overline{x}^{2^{n-1}} = \overline{1}$$

Ainsi, l'inverse de $\overline{x}$ est $\overline{x}^{2^{n-1}-1}$. L'algorithme de calcul est alors très simple.

Suivons maintenant la deuxième méthode proposée. On sait que x est impair (car premier avec 2^n) donc $x \equiv 1\,[2]$. On pose $y_1 = 1$. Supposons maintenant, pour $k \in \{1, \dots, n-1\}$, que l'on connait un entier y_k tel que $y_k x \equiv 1[2^k]$ (remarquons que $\overline{x}$ est inversible dans $\mathbb{Z}/2^k\mathbb{Z}$ car x est impair). Il existe donc un entier a tel que :

$$y_k x - 1 = 2^k a$$

Or x est impair donc il existe un entier b tel que $x + 1 = 2b$. Par produit, on en déduit que :

$$(y_k x - 1)(x + 1) = 2^{k+1} ab$$

ou encore :

$$y_k x^2 + y_k x - x - 1 = 2^{k+1} ab$$

En posant :

$$y_{k+1} = y_k x + y_k - 1$$

On a :

$$y_{k+1} x \equiv 1\,[2^{k+1}]$$

On obtient donc le schéma récursif suivant : $y_1 = 1$ et

$$\forall k \in \{1, \dots, n-1\},\ y_{k+1} = y_k x + y_k - 1$$

Alors $\overline{y_n}$ est l'inverse de $\overline{x}$ dans $\mathbb{Z}/2^n\mathbb{Z}$.

Exercice 12 –

1. Faux. Dans $\mathbb{Z}/8\mathbb{Z}$, $\overline{1}$, $\overline{3}$, $\overline{5}$ et $\overline{7}$ sont racines de $X^2 - \overline{1}$.
2. Faux. C'est vrai si et seulement si n est premier.
3. Faux. Dans $\mathbb{Z}/2\mathbb{Z}$, un seul élément est inversible.

3 Anneaux $\mathbb{K}[X]$

Dans ce chapitre, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$.

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

1. $X^3 + X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$. ☐ Vrai ☐ Faux
2. $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$. ☐ Vrai ☐ Faux
3. Un polynôme à coefficients réels irréductible dans $\mathbb{C}[X]$ l'est aussi dans $\mathbb{R}[X]$. ☐ Vrai ☐ Faux

Exercice 2 –

1. Rappeler, pour $n \geq 1$, la factorisation irréductible de $X^n - 1$ dans $\mathbb{C}$.
2. Donner la factorisation irréductible de $X^3 - 1$ dans $\mathbb{R}$.

Maîtriser les méthodes fondamentales

Exercice 3 –

Soit $A(X) = X^3 + 2X^2 - X - 2$ et $B(X) = X^2 + 4X + 3$.

1. Déterminer $A \wedge B$.
2. Trouver une relation de Bézout liée à A et B.

Exercice 4 –

Soit $B = X^3 - X^2 + X - 1$ et pour tout $n \in \mathbb{N}^*$,

$$A_n = (X^2 + X + 1)^n - X^{2n} - X^n - 1$$

1. Donner une condition nécessaire et suffisante sur n pour que B divise A_n.
2. Donner le reste de la division euclidienne de A_n par B.

Exercice 5 –

Soit $(I_n)_{n\geq 0}$ une suite croissante (pour l'inclusion) d'idéaux, non réduits au polynôme nul, de $\mathbb{C}[X]$. Montrer que $(I_n)_{n\geq 0}$ est stationnaire, c'est-à-dire qu'il existe un entier naturel n_0 tel que :

$$\forall n \geq n_0,\ I_n = I_{n_0}$$

Pour aller plus loin

Exercice 6 –

Un nombre complexe α est dit algébrique lorsqu'il est racine d'un polynôme non nul à coefficients entiers. Soit α un nombre algébrique.

1. Montrer l'existence d'un unique polynôme $\Pi \in \mathbb{Q}[X]$, unitaire et irréductible sur $\mathbb{Q}$, tel que $\Pi(\alpha) = 0$. On note d le degré de Π.
2. On pose :
$$\mathbb{Q}_{d-1}[\alpha] = \{P(\alpha),\ P \in \mathbb{Q}_{d-1}[X]\} \text{ et } \mathbb{Q}[\alpha] = \{P(\alpha),\ P \in \mathbb{Q}[X]\}$$
Montrer que $\mathbb{Q}[\alpha] = \mathbb{Q}_{d-1}[\alpha]$.
3. Montrer que $\mathbb{Q}_{d-1}[\alpha]$ est un corps.

Exercice 7 – Le vrai/faux de la fin

Soit $n \in \mathbb{N}^*$.

1. $(X^2+1)\mathbb{C}[X] + X\mathbb{C}[X] = \mathbb{C}[X]$. ☐ Vrai ☐ Faux
2. $(X^2-1)\mathbb{R}[X] + (X+1)\mathbb{R}[X] = \mathbb{R}[X]$. ☐ Vrai ☐ Faux
3. $(X^4+1)\mathbb{R}[X] \subset (X^2+\sqrt{2}X+1)\mathbb{R}[X]$. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. X^3+X^2+X+1 est irréductible dans $\mathbb{R}[X]$. ☐ Vrai ☒ Faux
2. X^2+X+1 est irréductible dans $\mathbb{R}[X]$. ☒ Vrai ☐ Faux
3. Un polynôme à coefficients réels irréductible dans $\mathbb{C}[X]$ l'est aussi dans $\mathbb{R}[X]$. ☒ Vrai ☐ Faux

🎓 Cours

Un polynôme P de $\mathbb{K}[X]$ est dit irréductible si il est non constant et si ses seuls diviseurs sont 1 et P, à constante multiplicative près. On a les résultats suivants :

- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.
- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Exercice 2 –

1. On a :

$$X^n - 1 = \prod_{k=0}^{n-1} (X - \mathrm{e}^{2ik\pi/n})$$

Cours

Tout polynôme non constant de $\mathbb{C}$ s'écrit comme un produit de polynômes de degré 1.

2. Remarquons que :

$\forall a, b \in \mathbb{R},\ a^3 - b^3 = (a-b)(a^2 + ab + b^2)$

$$X^3 - 1 = X^3 - 1^3 = (X-1)(X^2 + X + 1)$$

et $X^2 + X + 1$ n'admet que des racines complexes non réelles, ce qui donne le résultat.

Cours

Tout polynôme non constant de $\mathbb{R}[X]$ s'écrit comme un produit de polynômes de degré 1 et/ou de polynômes de degré 2 admettant des racines complexes non réelles conjuguées deux à deux.

Exercice 3 –

1. On applique l'algorithme d'Euclide :

- $X^3 + 2X^2 - X - 2 = (X^2 + 4X + 3)(X - 2) + 4X + 4$.
- $X^2 + 4X + 3 = (4X + 4)\left(\frac{X}{4} + \frac{3}{4}\right)$.

Le dernier reste non nul est $4X + 4$ et sachant que l'on souhaite obtenir un PGCD unitaire, on en déduit que :

$$(X^3 + 2X^2 - X - 2) \wedge (X^2 + 4X + 3) = X + 1$$

Méthode

Soit (A, B) un couple de polynômes non nuls tel que $\deg(A) \geq \deg(B)$.

- On pose $R_0 = A$ et $R_1 = B$.
- On définit R_2 comme étant le reste de la division euclidienne de R_0 par R_1.
- Si R_2 n'est pas nul, on définit R_3 comme étant le reste de la division euclidienne de R_1 par R_2 et ainsi de suite...
- La suite de terme général R_k créée de cette manière est donc une suite de polynômes dont les degrés décroissent strictement. Il existe alors un rang n tel que R_n soit le polynôme nul.
- Le polynôme R_{n-1} est alors un PGCD de A et B. Il suffit de le diviser par son coefficient dominant pour obtenir $A \wedge B$.

À retenir

On pouvait aussi factoriser les deux polynômes afin d'obtenir le PGCD.

2. D'après la question précédente, on a :

$$4X + 4 = X^3 + 2X^2 - X - 2 - (X - 2)(X^2 + 4X + 3)$$

Posons :

$$U(X) = \frac{1}{4} \text{ et } V(X) = \frac{1}{4}(2 - X)$$

On a alors :

$$A \wedge B = (X^3 + 2X^2 - X - 2)U(X) + (X^2 + 4X + 3)V(X)$$

Exercice 4 –

1. Supposons que B divise A_n. Sachant que 1 est racine de B alors 1 est racine de A_n donc $A_n(1)$ est nul et ainsi $3^n - 3 = 0$ donc $n = 1$. Réciproquement si $n = 1$ alors $A_1(X) = 0$ et B divise bien le polynôme nul. Ainsi, B divise A_n si et seulement si $n = 1$.

2. D'après le théorème de division euclidienne, il existe un unique couple $(Q_n, R_n) \in \mathbb{R}[X]^2$ tel que :

$$A_n = BQ_n + R_n$$

et vérifiant $\deg(R_n) < \deg(B) = 3$. Il existe donc $(a_n, b_n, c_n) \in \mathbb{R}^3$ tel que :

$$R_n(X) = a_nX^2 + b_nX + c_n$$

Les racines de B sont 1, i et $-i$.

$X^3 - X^2 + X - 1 = X^2(X - 1) + X - 1 = (X^2 + 1)(X - 1)$

A l'aide de l'égalité donnée par la division euclidienne, on obtient alors :

$$\begin{cases} a_n + b_n + c_n &= 3^n - 3 \\ -a_n + ib_n + c_n &= (-1)^{n+1} - 1 \\ -a_n - ib_n + c_n &= (-1)^{n+1} - 1 \end{cases}$$

A l'aide des opérations $L_3 \leftarrow L_3 - L_2$ et $L_2 \leftarrow L_2 + L_1$, le système est équivalent à :

$$\begin{cases} a_n + b_n + c_n &= 3^n - 3 \\ (1 + i)b_n + 2c_n &= 3^n + (-1)^{n+1} - 4 \\ -2ib_n &= 0 \end{cases}$$

En remontant les calculs, on obtient finalement :

$$R_n(X) = \frac{1}{2}\left((3^n + (-1)^n - 2)X^2 + 3^n + (-1)^{n+1} - 4\right)$$

Exercice 5 –

Soit $n \geq 0$. L'ensemble I_n est un idéal de $\mathbb{C}[X]$ et il n'est pas réduit au polynôme nul donc il existe un polynôme unitaire $P_n \in \mathbb{C}[X]$ tel que $I_n = P_n\mathbb{C}[X]$.

Cours

Tout idéal de I de $\mathbb{K}[X]$ est un idéal engendré par un élément de $\mathbb{K}[X]$. Si l'idéal contient un polynôme non nul, il existe de plus un unique polynôme P de $\mathbb{K}[X]$, normalisé, tel que $I = P\mathbb{K}[X]$.

La suite $(I_n)_{n\geq 0}$ est croissante donc pour tout entier naturel $n \geq 0$:

$$P_n\mathbb{C}[X] \subset P_{n+1}\mathbb{C}[X]$$

On en déduit que P_{n+1} divise P_n et en particulier :

$$\deg(P_{n+1}) \leq \deg(P_n)$$

On en déduit que la suite $(\deg(P_n))_{n\geq 0}$ est une suite d'entiers naturels décroissante donc stationnaire. Il existe donc un entier naturel n_0 tel que :

$$\forall n \geq n_0,\ \deg(P_n) = \deg(P_{n_0})$$

Or pour $n \geq n_0$, P_n divise P_{n_0} (car P_{k+1} divise P_k pour tout entier naturel k et par transitivité), P_{n_0} et P_n sont de même degré et unitaires donc $P_n = P_{n_0}$, ce qui donne le résultat :

$$\forall n \geq n_0,\ I_n = P_n\mathbb{C}[X] = P_{n_0}\mathbb{C}[X] = I_{n_0}$$

À retenir

Toute suite décroissante d'entiers naturels est stationnaire.

Exercice 6 –

1. Soit $\varphi : \mathbb{Q}[X] \to \mathbb{Q}$ l'application définie par :

$$\forall P \in \mathbb{Q}[X],\ \varphi(P) = P(\alpha)$$

Il est clair que φ est un morphisme d'anneaux donc le noyau de φ est un idéal de $\mathbb{Q}[X]$, et celui n'est pas réduit au polynôme nul car α est algébrique. Il existe donc un polynôme unitaire Π tel que le noyau de φ soit $\Pi\mathbb{Q}[X]$.

Le polynôme Π n'est pas nul (car unitaire) et n'est pas constant non nul (car α n'est pas racine d'un polynôme constant non nul) donc le degré de Π est au moins 1.

- Si ce degré vaut 1 alors Π est bien irréductible.
- Si le degré d de Π est supérieur ou égal à deux, supposons par l'absurde que Π n'est pas irréductible. Il existe alors deux polynômes P_1, P_2 de $\mathbb{Q}[X]$, ayant chacun un degré compris entre 1 et $d-1$ tels que $\Pi = P_1P_2$. Or $\Pi(\alpha) = 0$ donc $P_1(\alpha)P_2(\alpha) = 0$ et $\mathbb{Q}$ est un corps donc intègre donc $P_1(\alpha) = 0$ ou $P_2(\alpha) = 0$. On en déduit alors par définition de Π que P_1 ou P_2 est un multiple de Π ce qui est impossible pour des raisons de degré. Ainsi, Π est bien irréductible.

L'unicité de Π est claire (si $\tilde{\Pi}$ vérifie les mêmes propriétés, Π divise $\tilde{\Pi}$ et par irréductibilité et le fait que ces polynômes sont unitaires, on en déduit que $\Pi = \tilde{\Pi}$).

2. Il est clair que :

$$\mathbb{Q}_{d-1}[\alpha] \subset \mathbb{Q}[\alpha]$$

Soit $P \in \mathbb{Q}[X]$. Par division euclidienne, il existe un unique couple $(Q, R) \in \mathbb{Q}[X]^2$ tel que :

$$P = Q\Pi + R$$

et $\deg(R) < \deg(\Pi)$. On en déduit que :

$$P(\alpha) = Q(\alpha)\Pi(\alpha) + R(\alpha) = R(\alpha) \in \mathbb{Q}_{d-1}[\alpha]$$

car :

$$\deg(R) < \deg(\Pi) = d$$

On vient donc de montrer que :

$$\mathbb{Q}[\alpha] \subset \mathbb{Q}_{d-1}[\alpha]$$

ce qui prouve l'égalité par double inclusion.

3. D'après la question précédente, $\mathbb{Q}_{d-1}[\alpha] = \mathbb{Q}[\alpha]$ et il est clair que $\mathbb{Q}[\alpha]$ est l'image de $\mathbb{Q}[X]$ par le morphisme d'anneaux φ donc c'est un sous-anneau de $\mathbb{Q}$ donc un anneau. La commutativité est évidente.

Soit $P \in \mathbb{Q}_{d-1}[\alpha]$ tel que $P(\alpha) \neq 0$. Le polynôme Π est irréductible et de degré d et P a un degré strictement plus petit que d donc P et Π sont premier entre eux. D'après le théorème de Bézout, il existe deux polynômes A et B de $\mathbb{Q}[X]$ tels que :

$$AP + B\Pi = 1$$

On évalue alors en α :

$$A(\alpha)P(\alpha) = 1$$

donc :

$$\frac{1}{P(\alpha)} = A(\alpha) \in \mathbb{Q}[\alpha] = \mathbb{Q}_{d-1}[\alpha]$$

Ainsi, tout élément non nul de $\mathbb{Q}_{d-1}[\alpha]$ est inversible et son inverse appartient bien à $\mathbb{Q}_{d-1}[\alpha]$: cet ensemble est donc un corps.

Exercice 7 –

1. Vrai.

> **Cours**
>
> Soit $(P, Q) \in \mathbb{K}[X]^2$. On appelle PGCD de P et Q le générateur normalisé de l'idéal $P\mathbb{K}[X] + Q\mathbb{K}[X]$. On le note $P \wedge Q$. On a donc en particulier :
>
> $$P\mathbb{K}[X] + Q\mathbb{K}[X] = (P \wedge Q)\mathbb{K}[X]$$

2. Faux. Le PGCD de $X^2 - 1$ et $X + 1$ est $X + 1$ et $(X + 1)\mathbb{R}[X]$ est différent de $\mathbb{R}[X]$.

3. Vrai. Une division euclidienne permet de montrer que :

$$X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$$

4 Compléments d'algèbre linéaire

Dans ce chapitre, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ et n un entier naturel non nul.

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

Soit $E = \mathbb{R}^3$, $x = (1, 1, 0)$, $y = (0, 1, 1)$ et $z = (1, 2, 1)$.

1. Vect(x) et Vect(y) sont en somme directe. ☐ Vrai ☐ Faux

2. Vect(x) et Vect(y) sont supplémentaires dans E. ☐ Vrai ☐ Faux

3. Vect(x),Vect(y) et Vect(z) sont en somme directe. ☐ Vrai ☐ Faux

Exercice 2 –

Calculer le déterminant de la matrice suivante :

$$A = \begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 3 & 6 & 5 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

Exercice 3 –

Soit E un espace vectoriel de dimension 5 et $\mathscr{B} = (e_1, e_2, e_3, e_4, e_5)$ une base de E. On suppose que la matrice d'un endomorphisme u de E dans la base $\mathscr{B}$ est de la forme :

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 5 & 7 \end{pmatrix}$$

Que peut-on dire de $F = \text{Vect}(e_1, e_2, e_3)$?

Maîtriser les méthodes fondamentales

Exercice 4 –

Montrer que le sous-espace vectoriel des matrices symétriques $S_n(\mathbb{R})$ et celui des matrices antisymétriques $A_n(\mathbb{R})$ sont supplémentaires dans $\mathscr{M}_n(\mathbb{R})$.

Exercice 5 –

Soit $F = \{(x+y, y-2x, x),\ (x,y) \in \mathbb{R}^2\}$ et $G = \text{Vect}((1,1,1))$. Montrer que F et G sont supplémentaires dans $\mathbb{R}^3$.

Exercice 6 –

Soit E un espace vectoriel et f un endomorphisme de E. On pose :

$$\forall k \in [\![1\,;\,3]\!],\ E_k = \text{Ker}(f - k\text{Id}_E)$$

Montrer que E_1, E_2 et E_3 sont en somme directe.

Exercice 7 –

Soit $A, B \in \mathcal{M}_n(\mathbb{K})$. Montrer que :

$$\begin{vmatrix} A & B \\ B & A \end{vmatrix} = \det(A+B)\det(A-B)$$

Pour aller plus loin

Exercice 8 –

Soit $E = \mathcal{F}(\mathbb{R},\mathbb{R})$. Montrer que le sous-espace vectoriel de E constitué des fonctions affines est un supplémentaire du sous-espace vectoriel F de E défini par $F = \{f \in E,\ f(0) = f(1) = 0\}$.

Exercice 9 –

Soit E l'espace des fonctions continues sur $[-1,1]$ et à valeurs dans $\mathbb{R}$. On considère les sous-espaces vectoriels suivants de E :

$$F_1 = \{f \in E,\ f \text{ est constante}\}$$
$$F_2 = \{f \in E,\ \forall t \in [-1,0],\ f(t) = 0\}$$
$$F_3 = \{f \in E,\ \forall t \in [0,1],\ f(t) = 0\}$$

Montrer que $E = F_1 \oplus F_2 \oplus F_3$.

Exercice 10 –

Considérons E un $\mathbb{K}$-espace vectoriel de dimension finie. Montrer que si F et G sont deux sous-espaces vectoriels de E de même dimension alors ils ont un sous-espace supplémentaire en commun.

Exercice 11 – Le vrai/faux de la fin

Soit E un espace vectoriel de dimension finie n et $F_1, \dots, F_p$ des sous-espaces vectoriels de E ($p \geq 2$).

1. $\dim(F_1 + \cdots + F_p) \leq \sum_{i=1}^{p} \dim(F_i)$. ☐ Vrai ☐ Faux

2. Si $\sum_{i=1}^{p} \dim(F_i) = n$ alors $E = F_1 \oplus \cdots \oplus F_p$. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. $\text{Vect}(x) \cap \text{Vect}(y) = \{(0,0,0)\}$.	☒ Vrai	☐ Faux
2. $\dim(\text{Vect}(x)) + \dim(\text{Vect}(y)) = 2 < \dim(E)$.	☐ Vrai	☒ Faux
3. $z = x + y$.	☐ Vrai	☒ Faux

🎓 Cours

Soit E un $\mathbb{K}$-espace vectoriel et $E_1, E_2, \dots, E_p$ des sous-espaces vectoriels de E.

- On définit la *somme* de ces sous-espaces par :

$$\sum_{k=1}^{p} E_k = \left\{ \sum_{k=1}^{p} x_k,\ (x_1, x_2, \dots, x_p) \in E_1 \times E_2 \times \cdots \times E_p \right\}$$

  La somme de ces sous-espaces vectoriels est un sous-espace vectoriel de E.

- On dit que la somme $\sum_{k=1}^{p} E_k$ est *directe* si :

$$\forall (x_1, x_2, \dots, x_p) \in E_1 \times E_2 \times \cdots \times E_p,\ \sum_{k=1}^{p} x_k = 0_E \Longrightarrow \forall k \in \{1, \dots p\},\ x_k = 0_E$$

  Dans ce cas, la somme se note $\bigoplus_{k=1}^{p} E_k = E_1 \oplus \cdots \oplus E_p$.

- La somme $\sum_{k=1}^{p} E_k$ est directe si et seulement si tout élément x de $\sum_{k=1}^{p} E_k$ se décompose de manière *unique* sous la forme :

$$x = x_1 + x_2 + \dots + x_p$$

  où pour tout $k \in \{1, \dots, p\}$, $x_k \in E_k$.

Exercice 2 –

Un calcul de déterminant par blocs montre que :

$$\det(A) = \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} \times \begin{vmatrix} 2 & 3 \\ 1 & 3 \end{vmatrix}$$

donc $\det(A) = 1 \times 3 = 3$.

Cours

Soit A une matrice carrée de la forme :

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

où B et D sont des matrices carrées. Alors :

$$\det(A) = \det(B)\det(D)$$

Exercice 3 –

On remarque que M est une matrice triangulaire par blocs. Il est clair que :

$$\forall i \in [\![1\,;\,3]\!],\ u(e_i) \in \mathrm{Vect}(e_1, e_2, e_3) = F$$

On en déduit que F est un sous-espace vectoriel stable par u.

Exercice 4 –

Raisonnons par analyse-synthèse.

Analyse. Supposons que $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$. Soit $M \in \mathcal{M}_n(\mathbb{R})$. Il existe un unique couple (S, A) appartenant à $\mathcal{S}_n(\mathbb{R}) \times \mathcal{A}_n(\mathbb{R})$ tel que $M = S + A$. Par linéarité de la transposition, on a alors :

$$M^T = S^T + A^T = S - A$$

Ainsi :

$$M + M^T = 2S \ \text{ et } \ M - M^T = 2A$$

donc :

$$S = \frac{M + M^T}{2} \ \text{ et } \ A = \frac{M - M^T}{2}$$

Synthèse. Soit $M \in \mathcal{M}_n(\mathbb{R})$. Posons :

$$S = \frac{M + M^T}{2} \ \text{ et } \ A = \frac{M - M^T}{2}$$

Il est évident que $M = S + A$. On a :

Linéarité de la transposition

$$S^T = \frac{M^T + (M^T)^T}{2} = \frac{M^T + M}{2} = S$$

Ainsi, S est symétrique. De même, A est antisymétrique. Ainsi $\mathcal{M}_n(\mathbb{R}) \subset \mathcal{S}_n(\mathbb{R}) + \mathcal{A}_n(\mathbb{R})$ et l'autre inclusion est vérifiée car $\mathcal{S}_n(\mathbb{R})$ et $\mathcal{A}_n(\mathbb{R})$ sont des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{R})$. Finalement, $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) + \mathcal{A}_n(\mathbb{R})$. De plus, d'après l'analyse, toute matrice s'écrit de manière unique comme la somme d'une matrice symétrique et d'une matrice antisymétrique donc la somme est directe. Ainsi, $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}_n(\mathbb{R}) \oplus \mathcal{A}_n(\mathbb{R})$.

Méthode

Soit F et G deux sous-espaces vectoriels d'un espace vectoriel E. Montrer que F et G sont supplémentaires dans E par analyse-synthèse se fait en suivant la démarche suivante :

- Dans l'analyse, on suppose que tout vecteur x de E s'écrit sous la forme $x_F + x_G$ où x_F appartient à F et x_G appartient à G. En utilisant l'appartenance de ces deux vecteurs aux sous-espaces F et G, on obtient l'expression de x_F (ou de x_G) en fonction de x uniquement. L'égalité $x = x_F + x_G$ permet d'obtenir l'autre vecteur en fonction de x. Cette phase d'analyse montre l'*unicité* de la décomposition d'un vecteur de E comme la somme d'un élément de F et d'un élément de G si *existence*.
- Dans la synthèse, on prouve effectivement l'existence d'une telle décomposition. On fixe x un vecteur de E et on définit x_F et x_G comme obtenus dans l'analyse. On montre alors que x_F appartient à F, x_G appartient à G et que $x_F + x_G = x$.

Exercice 5 –

G est un sous-espace vectoriel de dimension 1 car $(1, 1, 1)$ est non nul. On a :

$$\begin{aligned} F &= \{(x + y, y - 2x, x),\ (x, y) \in \mathbb{R}^2\} \\ &= \{x(1, -2, 1) + y(1, 1, 0),\ (x, y) \in \mathbb{R}^2\} \\ &= \text{Vect}((1, -2, 1), (1, 1, 0)) \end{aligned}$$

Ainsi, F est un sous-espace vectoriel de dimension 2 car $(1, -2, 1)$ et $(1, 1, 0)$ sont non colinéaires donc forment une famille libre.

On a donc :

$$\dim(F) + \dim(G) = \dim(\mathbb{R}^3)$$

Montrons que $F \cap G = \{(0, 0, 0)\}$. L'inclusion $\{(0, 0, 0)\} \subset F \cap G$ est claire car F et G sont des sous-espaces vectoriels de $\mathbb{R}^3$. Soit $X \in F \cap G$. Le vecteur X appartient à G donc il existe un réel a tel que :

$$X = a(1, 1, 1)$$

Le vecteur X appartient à F donc il existe deux réels x et y tels que :

$$X = (x + y, y - 2x, x)$$

Ainsi, $x + y = a$, $y - 2x = a$ et $x = a$.

En utilisant que $x = a$, on obtient avec les deux premières égalités $y = 0$ et $y = 2x + a = 3a$. Alors $3a = 0$ donc $a = 0$ et finalement $X = (0, 0, 0)$. On en déduit $F \cap G \subset \{(0, 0, 0)\}$ et ainsi l'égalité. On a donc :

$$\dim(F) + \dim(G) = \dim(\mathbb{R}^3) \quad \text{et} \quad F \cap G = \{(0, 0, 0)\}$$

Les sous-espaces vectoriels F et G sont donc supplémentaires dans $\mathbb{R}^3$.

À retenir

Pas besoin d'analyse-synthèse si l'on souhaite juste prouver que deux sous-espaces vectoriels, d'un espace de dimension finie, sont supplémentaires.

Exercice 6 –

Soit $(x_1, x_2, x_3) \in E_1 \times E_2 \times E_3$ tel que :

$$x_1 + x_2 + x_3 = 0_E$$

On a alors :

$$f(x_1 + x_2 + x_3) = f(0_E)$$

donc : *f est une application linéaire*

$$f(x_1) + f(x_2) + f(x_3) = 0_E$$

Or, pour $k \in [\![1\,;\,3]\!]$, x_k appartient à $\mathrm{Ker}(f - k\mathrm{Id}_E)$ donc $f(x_1) = x_1$, $f(x_2) = 2x_2$ et $f(x_3) = 3x_3$. On en déduit que :

$$x_1 + 2x_2 + 3x_3 = 0_E$$

On réitère le procédé précédent :

$$f(x_1 + 2x_2 + 3x_3) = f(0_E)$$

puis par linéarité de f :

$$f(x_1) + 2f(x_2) + 3f(x_3) = 0_E$$

et finalement :

$$x_1 + 4x_2 + 9x_3 = 0_E$$

On souhaite alors résoudre le système suivant :

$$\begin{cases} x_1 + x_2 + x_3 &= 0_E \\ x_1 + 2x_2 + 3x_3 &= 0_E \\ x_1 + 4x_2 + 9x_3 &= 0_E \end{cases}$$

Les opérations $L_2 \leftarrow L_2 - L_1$ et $L_3 \leftarrow L_3 - L_1$ permettent d'obtenir :

$$\begin{cases} x_1 + x_2 + x_3 &= 0_E \\ x_2 + 2x_3 &= 0_E \\ 3x_2 + 8x_3 &= 0_E \end{cases}$$

On utilise maintenant l'opération $L_3 \leftarrow L_3 - 3L_2$:

$$\begin{cases} x_1 + x_2 + x_3 &= 0_E \\ x_2 + 2x_3 &= 0_E \\ 2x_3 &= 0_E \end{cases}$$

En remontant les calculs, on obtient alors $x_3 = 0_E$ puis $x_2 = 0_E$ et finalement $x_1 = 0_E$. On en déduit que E_1, E_2 et E_3 sont en somme directe.

Méthode

Pour résoudre un système linéaire, l'algorithme du pivot de Gauss doit être privilégié pour gagner en efficacité sauf si il y a des équations incomplètes permettant des substitutions efficaces.

Exercice 7 –

Par opération sur les colonnes $C_i \leftarrow C_i + C_{n+i}$ pour $i \in [\![1\,;\,n]\!]$, on a :

$$\begin{vmatrix} A & B \\ B & A \end{vmatrix} = \begin{vmatrix} A+B & B \\ B+A & A \end{vmatrix}$$

puis par opérations sur les lignes $L_{i+n} \leftarrow L_{i+n} - L_i$ pour $i \in [\![1\,;\,n]\!]$:

$$\begin{vmatrix} A & B \\ B & A \end{vmatrix} = \begin{vmatrix} A+B & B \\ 0 & A-B \end{vmatrix} = \det(A+B)\det(A-B)$$

par calcul du déterminant par blocs.

Exercice 8 –

À retenir

On montre facilement que l'ensemble des fonctions affines est un sous-espace vectoriel de E à l'aide de la méthode des trois points ou en l'identifiant à $\mathbb{R}_1[X]$.

Notons A le sous-espace vectoriel de E constitué des fonctions affines et θ l'application nulle de E. Raisonnons par analyse-synthèse.

Analyse. Supposons que $E = A \oplus F$. Soit $f \in E$. Il existe alors $(g, h) \in A \times F$ tel que $f = g + h$. Ainsi, pour tout $x \in \mathbb{R}$,

$$f(x) = g(x) + h(x)$$

La fonction g est affine donc il existe deux réels a et b tels que pour tout réel x,

$$g(x) = ax + b$$

donc :

$$f(x) = ax + b + h(x)$$

La fonction h appartient à F donc $h(0) = h(1) = 0$ ce qui implique que :

$$f(0) = b$$

et

$$f(1) = a + b$$

Ainsi, $b = f(0)$ et $a = f(1) - f(0)$. On a donc pour tout $x \in \mathbb{R}$,

$$g(x) = (f(1) - f(0))x + f(0)$$

et $h = f - g$.

Synthèse. Soit $f \in E$. Posons pour tout $x \in \mathbb{R}$,

$$g(x) = (f(1) - f(0))x + f(0) \quad \text{et} \quad h(x) = f(x) - g(x)$$

On a $f = g + h$. La fonction g appartient à A. On a :

g est clairement affine

$$h(0) = f(0) - g(0) = f(0) - f(0) = 0$$

et

$$h(1) = f(1) - g(1) = f(1) - (f(1) - f(0) + f(0)) = 0$$

Ainsi, h appartient à F.

Toute fonction de E s'écrit donc comme la somme d'une fonction de A et d'une fonction de F. L'analyse prouve que cette décomposition est unique. Ainsi, A et F sont supplémentaires dans E.

Exercice 9 –

Raisonnons par analyse-synthèse.

Analyse. Supposons que $E = F_1 \oplus F_2 \oplus F_3$. Soit $f \in E$. Il existe donc $(f_1, f_2, f_3) \in F_1 \times F_2 \times F_3$ tel que :

$$f = f_1 + f_2 + f_3$$

La fonction f_1 est constante donc il existe un réel c tel que pour tout $t \in [-1, 1]$, $f_1(t) = c$. On a donc pour $t \in [-1, 1]$,

$$f(t) = c + f_2(t) + f_3(t)$$

Les fonctions f_2 et f_3 appartiennent à F_2 et F_3 donc :

$$f(0) = c + f_2(0) + f_3(0) = c$$

Sachant que f_2 appartient à F_2, on a pour tout $t \in [-1, 0[$:

$$f(t) = c + 0 + f_3(t) = f(0) + f_3(t)$$

donc

$$f_3(t) = f(t) - f(0)$$

De même, on obtient que pour tout $t \in]0, 1]$,

$$f_2(t) = f(t) - f(0)$$

Synthèse. Soit $f \in E$. Posons pour tout $t \in [-1, 1]$, $f_1(t) = f(0)$,

$$f_2(t) = \begin{cases} 0 & \text{si } t \in [-1, 0] \\ f(t) - f(0) & \text{si } t \in]0, 1] \end{cases} \quad \text{et} \quad f_3(t) = \begin{cases} f(t) - f(0) & \text{si } t \in [-1, 0[\\ 0 & \text{si } t \in [0, 1] \end{cases}$$

La fonction f_1 est constante sur $[-1, 1]$ donc appartient à F_1.

La fonction f_2 appartient bien à E car est continue sur $[-1, 0[$, sur $]0, 1]$ et sachant que f est continue en 0 :

Ne pas oublier de vérifier la continuité !

$$\lim_{t \to 0^-} f_2(t) = \lim_{t \to 0^+} f_2(t) = f_2(0) = 0$$

De plus pour tout $t \in [-1, 0]$, $f_2(t) = 0$. Ainsi, f_2 appartient à F_2. On prouve de même que f_3 appartient à F_3.

Pour tout $t \in [-1, 0[$,

$$f_1(t) + f_2(t) + f_3(t) = f(0) + 0 + f(t) - f(0) = f(t)$$

On obtient le même résultat si $t \in]0, 1]$. Pour finir,

$$f_1(0) + f_2(0) + f_3(0) = f(0) + 0 + 0 = f(0)$$

Ainsi, $f = f_1 + f_2 + f_3$.

Finalement, tout fonction de E s'écrit comme la somme de trois fonctions de F_1, F_2 et F_3. Cette décomposition est unique d'après l'analyse. Ainsi, $E = F_1 \oplus F_2 \oplus F_3$.

Exercice 10 –

Notons n la dimension de E et r la dimension commune de F et G. Nous raisonnons par récurrence descendante.

- Si $r = n$, le résultat est évident : on peut choisir comme supplémentaire commun $H = \{0_E\}$.
- Soit r strictement plus petit que n et supposons la propriété vérifiée pour tous les couples de sous-espaces de dimension $r + 1$. Une propriété classique énonce que la réunion de deux sous-espaces vectoriels A et B de E est un sous-espace vectoriel de E si et seulement si $A \subset B$ ou $B \subset A$. Dans notre cas, la réunion de F et G ne peut donc être égale à E que si $F = G = E$ ce qui n'est pas le cas vu l'hypothèse sur les dimensions. Ainsi, il existe un vecteur non nul x de E tel que $x \notin F \cup G$. Comme x n'appartient, ni à F, ni à G, les sous-espaces $\tilde{F} = F \oplus \text{Vect}(x)$ et $\tilde{G} = G \oplus \text{Vect}(x)$ sont de dimensions $r + 1$ et ont donc par hypothèse de récurrence un supplémentaire en commun que l'on note $\tilde{H}$. Ainsi :

  $$F \oplus \text{Vect}(x) \oplus \tilde{H} = G \oplus \text{Vect}(x) \oplus \tilde{H} = E$$

  Le sous-espace $H = \text{Vect}(x) \oplus \tilde{H}$ est alors un supplémentaire commun à F et G.

On a donc bien démontré le résultat par récurrence descendante sur r.

À retenir

Soit F, G deux sous-espaces vectoriels d'un espace vectoriel E. Alors $F \cup G$ est un sous-espace vectoriel de E si et seulement si $F \subset G$ ou $G \subset F$.

Exercice 11 –

1. Vrai. C'est une propriété de cours.
2. Faux. Il suffit de penser à un contre-exemple où $F_1 = \cdots = F_p$ avec $p = n$.

5 Éléments propres

Dans ce chapitre, $\mathbb{K}$ désignera $\mathbb{R}$ ou $\mathbb{C}$ et n un entier naturel non nul.

Maîtriser le cours

Exercice 1 – Le vrai/faux du début

Soit E un $\mathbb{K}$-espace vectoriel, u un endomorphisme de E, $x \in E$ et $\lambda \in \mathbb{K}$.

1. Si $u(x) = \lambda x$ alors x est un vecteur propre de u. ☐ Vrai ☐ Faux
2. Si $u(x) = \lambda x$ et $\lambda \neq 0$ alors x est un vecteur propre de u. ☐ Vrai ☐ Faux
3. Si x est non nul et appartient à $\mathrm{Ker}(u - \lambda \mathrm{Id}_E)$ alors x est un vecteur propre de u. ☐ Vrai ☐ Faux

Exercice 2 –

Soit $E = \mathscr{C}^\infty(\mathbb{R}, \mathbb{R})$ et D l'endomorphisme de E défini par :

$$\forall f \in E,\ D(f) = f'$$

Justifier que tout réel λ est valeur propre pour D et donner un vecteur propre associé.

Exercice 3 –

Soit u et v deux endomorphismes d'un $\mathbb{K}$-espace vectoriel E qui commutent.

1. Montrer que l'image de u est stable par v.
2. Montrer que le noyau de u est stable par v.
3. Montrer que tout sous-espace propre de u est stable par v.

Exercice 4 –

Soit $A \in \mathscr{M}_n(\mathbb{R})$ une matrice telle que la somme des coefficients de chaque ligne est égale à une constante $c \in \mathbb{R}$. Montrer que c est valeur propre de A et déterminer un vecteur propre associé.

Maîtriser les méthodes fondamentales

Exercice 5 –

Soit $E = \mathbb{K}[X]$ et u l'endomorphisme de E défini par $u(P(X)) = XP(X)$ pour $P \in E$. Déterminer les (éventuelles) valeurs propres de u en raisonnant par analyse-synthèse.

Exercice 6 –
Soit f un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie. On suppose que 0 est dans le spectre de f^n. Montrer que 0 est aussi dans le spectre de f.

Exercice 7 –
Soit E l'espace vectoriel des fonctions de classe $\mathscr{C}^\infty$ définies sur $\mathbb{R}$ à valeurs dans $\mathbb{R}$.
Montrer que $\{f_a : x \mapsto \cos(ax),\ a \in \mathbb{R}_+\}$ est une famille libre de E.

Pour aller plus loin

Exercice 8 –
Soit $E = \mathbb{R}[X]$ et $\varphi \in \mathscr{L}(E)$ défini par :

$$\forall P \in E,\ \varphi(P) = XP'$$

Déterminer les éléments propres de φ.

Exercice 9 –
Soit $E = \mathscr{C}(\mathbb{R}_+, \mathbb{R})$. On définit T qui à $f \in E$, associe $T(f) : \mathbb{R}_+ \to \mathbb{R}$ définie par :

$$\forall x > 0,\ T(f)(x) = \frac{1}{x}\int_0^x f(t)\mathrm{d}t$$

et $T(f)(0) = f(0)$.

1. Montrer que T est un endomorphisme de E.
2. Déterminer les éléments propres de T.
3. T est-il injectif?
4. T est-il surjectif?

Exercice 10 – Le vrai/faux de la fin
Soit $A \in \mathscr{M}_3(\mathbb{R})$ définie par :

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 0 & 3 \\ 3 & -3 & 4 \end{pmatrix}$$

1. 2 est valeur propre de A. ☐ Vrai ☐ Faux
2. 0 est valeur propre de A. ☐ Vrai ☐ Faux
3. 1, 2, 3 et 4 sont valeurs propres de A. ☐ Vrai ☐ Faux

Solution des exercices

Exercice 1 –

1. Si $u(x) = \lambda x$ alors x est un vecteur propre de u. ☐ Vrai ☒ Faux
2. Si $u(x) = \lambda x$ et $\lambda \neq 0$ alors x est un vecteur propre de u. ☐ Vrai ☒ Faux
3. Si x est non nul et appartient à $\mathrm{Ker}(u - \lambda \mathrm{Id}_E)$ alors x est un vecteur propre de u. ☒ Vrai ☐ Faux

🎓 Cours

Soit $u \in \mathscr{L}(E)$.

- Un scalaire $\lambda \in \mathbb{K}$ est appelé *valeur propre* de u s'il existe un vecteur x de E, *non nul*, tel que $u(x) = \lambda x$.
- Un vecteur x de E est appelé *vecteur propre* de u s'il est *non nul* et s'il existe un scalaire $\lambda \in \mathbb{K}$ tel que $u(x) = \lambda x$.
- Soit λ une valeur propre de $u \in \mathscr{L}(E)$. On appelle *sous-espace propre* de u associé à la valeur propre λ, le sous-espace vectoriel noté $E_\lambda(u)$ défini par $E_\lambda(u) = \mathrm{Ker}(u - \lambda \mathrm{Id}_E)$. Les vecteurs *non nuls* de $E_\lambda(u)$ sont les vecteurs propres de u associés à la valeur propre λ.

Exercice 2 –

Soit $\lambda \in \mathbb{R}$. Posons f l'élément de E défini par :

$$\forall x \in \mathbb{R},\ f(x) = \mathrm{e}^{\lambda x}$$

Alors f est une fonction non nulle et il est clair que $D(f) = \lambda f$ donc f est un vecteur propre de D associé à la valeur propre λ.

Exercice 3 –

1. Montrons que $\mathrm{Im}(u)$ est stable par v, c'est-à-dire :

$$\forall y \in \mathrm{Im}(u),\ v(y) \in \mathrm{Im}(u)$$

Soit $y \in \mathrm{Im}(u)$. Il existe $x \in E$ tel que $y = u(x)$. Ainsi :

$$\begin{aligned} v(y) &= v(u(x)) \\ &= v \circ u(x) \\ &= u \circ v(x) \ \text{ car } u \circ v = v \circ u \\ &= u(v(x)) \end{aligned}$$

avec $v(x) \in E$. Ainsi, $v(y) \in \mathrm{Im}(u)$. On a donc montré le résultat souhaité.

Cours

Soit $u \in \mathscr{L}(E)$ et F un sous-espace vectoriel de E. On dit que F est *stable* par u si $u(F) \subset F$ ou autrement dit si :

$$\forall x \in F,\ u(x) \in F$$

2. Montrons que $\mathrm{Ker}(u)$ est stable par v, c'est-à-dire :

$$\forall x \in \mathrm{Ker}(u),\ v(x) \in \mathrm{Ker}(u)$$

Soit $x \in \mathrm{Ker}(u)$. Alors :

$$\begin{aligned} u(v(x)) &= u \circ v(x) \\ &= v \circ u(x) \quad \text{car } u \circ v = v \circ u \\ &= v(u(x)) \\ &= v(0_E) \qquad \text{car } x \in \mathrm{Ker}(u) \\ &= 0_E \qquad\ \ \text{car } v \in \mathscr{L}(E) \end{aligned}$$

Ainsi, $v(x) \in \mathrm{Ker}(u)$. On a bien montré le résultat souhaité.

3. Soit $\lambda \in \mathbb{K}$. Montrons que $E_\lambda(u)$ est stable par v. Par hypothèse, u commute avec v. De plus, Id_E commute aussi avec v donc $u - \lambda \mathrm{Id}_E$ commute avec v. D'après la question précédente, on en déduit que $E_\lambda(u) = \mathrm{Ker}(u - \lambda \mathrm{Id}_E)$ est stable par v.

À retenir

Les trois propriétés précédentes sont importantes, il est important de savoir les citer et les prouver.

Exercice 4 –

Soit $X \in \mathscr{M}_{n,1}(\mathbb{R})$ défini par :

$$X = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

Alors X est un vecteur non nul et par hypothèse, on a :

Ne pas oublier de dire que X est non nul

$$AX = \begin{pmatrix} c \\ c \\ \vdots \\ c \end{pmatrix} = cX$$

Ainsi, X est un vecteur propre de A associé à la valeur propre c.

Cours

Soit $A \in \mathcal{M}_n(\mathbb{K})$.

- Un scalaire $\lambda \in \mathbb{K}$ est une *valeur propre* de A s'il existe un vecteur X de $\mathcal{M}_{n,1}(\mathbb{K})$ *non nul* tel que $AX = \lambda X$.
- Un vecteur X de $\mathcal{M}_{n,1}(\mathbb{K})$ est un *vecteur propre* de A s'il est *non nul* et s'il existe un scalaire $\lambda \in \mathbb{K}$ tel que $AX = \lambda X$.
- Le *spectre* de A est l'ensemble de ses valeurs propres.
- Le *sous-espace propre* associé à la valeur propre de A, que l'on notera $E_\lambda(A)$, est défini par :

$$E_\lambda(A) = \mathrm{Ker}(A - \lambda \mathrm{I}_n)$$

C'est un sous-espace vectoriel de $\mathcal{M}_{n,1}(\mathbb{K})$ dont les éléments non nuls sont les vecteurs propres de A associés à la valeur propre λ.

Exercice 5 –

Raisonnons par analyse-synthèse.

Analyse. Supposons l'existence d'un scalaire λ, valeur propre de u. Par définition, il existe un vecteur P non nul tel que $u(P(X)) = \lambda P(X)$ et donc par définition de u, $XP(X) = \lambda P(X)$ ou encore :

$$(X - \lambda)P(X) = 0$$

Or $(X - \lambda)$ est un polynôme non nul donc $P(X) = 0$ ce qui est absurde. $\mathbb{K}[X]$ est intègre

Synthèse. Le raisonnement précédent montre que l'endomorphisme u n'admet pas de valeur propre.

Méthode

Dans le cas où l'on étudie un endomorphisme d'un espace vectoriel de dimension infinie, il est fréquent d'utiliser un raisonnement par analyse-synthèse.

Exercice 6 –

Supposons que 0 est dans le spectre de f^n. Alors le noyau de f^n n'est pas réduit au vecteur nul donc f^n n'est pas injective donc n'est pas bijective donc son déterminant est nul. Or :

$$\det(f^n) = \det(f)^n$$

On en déduit que $\det(f)$ est nul donc f n'est pas bijective et ainsi f n'est pas injective (l'espace vectoriel est de dimension finie) et 0 est valeur propre de f.

À retenir

Soit $u \in \mathcal{L}(E)$. Les assertions suivantes sont équivalentes :

- Le scalaire 0 est valeur propre de u.
- $\mathrm{Ker}(u) \neq \{0_E\}$.
- L'application u n'est pas injective.

Exercice 7 –

Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_n$ des réels distincts. Montrons que $(f_{a_1}, \dots, f_{a_n})$ est une famille libre de E. Posons $\mathscr{D}$ l'endomorphisme de E défini par $\mathscr{D}(f) = f''$. On a pour tout $i \in [\![1\,;\,n]\!]$, $\mathscr{D}(f_{a_i}) = -a_i^2 f_{a_i}$ et ainsi f_{a_i} (qui n'est pas la fonction nulle) est un vecteur propre de $\mathscr{D}$ associée à la valeur propre $-a_i^2$. Les réels positifs $a_1, \dots, a_n$ étant distincts, et la fonction $x \mapsto -x^2$ étant injective sur $\mathbb{R}_+$, les réels $-a_1^2, \dots, -a_n^2$ sont aussi distincts donc la famille $(f_{a_1}, \dots, f_{a_n})$ est une famille de vecteurs propres associés à des valeurs propres deux à deux distinctes d'un endomorphisme u de E et est donc une famille libre de E.

Cours

Une famille de vecteurs propres associés à des valeurs propres deux à deux distinctes d'un endomorphisme u de E est une famille libre de E.

Exercice 8 –

Raisonnons par analyse-synthèse.

Analyse. Soit $\lambda \in \mathbb{R}$ une valeur propre de φ. Il existe donc un polynôme non nul de E tel que $\varphi(P) = \lambda P$ ou encore $XP' = \lambda P$. On a donc pour tout réel x :

$$xP'(x) = \lambda P(x)$$

En particulier, P est solution sur $\mathbb{R}_+^*$ de l'équation différentielle linéaire homogène du premier ordre suivante :

$$y' - \frac{\lambda}{x} y = 0$$

dont les solutions sont de la forme :

$$x \mapsto K\mathrm{e}^{\lambda \ln(x)} = Kx^\lambda$$

où $K \in \mathbb{R}$. Si λ n'est pas un entier naturel, toutes les dérivées successives de $x \mapsto x^\lambda$ sont non nulles car pour tout entier $n \geq 0$, la dérivée n-ième de $x \mapsto x^\lambda$ a pour expression :

$$\lambda(\lambda - 1) \times \cdots (\lambda - n + 1) x^{\lambda - n}$$

ce qui est impossible car P est un polynôme donc à partir d'un certain rang, toutes ses dérivées sont nulles. Si λ est un entier naturel que l'on renomme n, on en déduit que :

$$\forall x > 0,\ P(x) = Kx^n$$

où $K \in \mathbb{R}$ donc $P = KX^n$.

Deux polynômes coïncidant en une infinité de valeurs sont égaux

Synthèse. On a $\varphi(1) = 0$ et pour tout entier $n \geq 1$,

$$\varphi(X^n) = X(X^n)' = X(nX^{n-1}) = nX^n$$

Pour tout entier $n \geq 0$, X^n est non nul et on en déduit que c'est un vecteur propre de φ associé à la valeur propre n.

D'après l'analyse-synthèse, on sait que le spectre de φ est $\mathbb{N}$ et que pour tout entier $n \geq 0$,

$$E_n(\varphi) = \mathrm{Vect}(X^n)$$

Exercice 9 –

1. Soit $f \in E$. Montrons que $T(f)$ appartient à E. Soit F une primitive de f sur $\mathbb{R}_+$ (qui existe car f est continue sur cet intervalle). Pour tout $x > 0$, on a :

$$T(f)(x) = \frac{F(x) - F(0)}{x} = \frac{F(x) - F(0)}{x - 0}$$

On en déduit que $T(f)$ est $\mathscr{C}^1$ (donc en particulier continue) sur $\mathbb{R}_+^*$. De plus, la fonction F est dérivable en 0 et $F'(0) = f(0)$ donc :

$$\lim_{x \to 0} \frac{F(x) - F(0)}{x - 0} = f(0)$$

et ainsi :

$$\lim_{x \to 0} T(f)(x) = T(f)(0)$$

On en déduit que $T(f)$ est continue en 0 et finalement sur $\mathbb{R}_+$. Ainsi :

$$\forall f \in E,\ T(f) \in E$$

À retenir

Toute fonction continue sur un intervalle, et à valeurs réelles, admet une primitive sur celui-ci.

Montrons la linéarité de T. Soit $f, g \in E$ et $\lambda \in \mathbb{R}$. Pour tout réel $x > 0$, on a par linéarité de l'intégrale :

$$T(\lambda f + g)(x) = \frac{1}{x}\int_0^x (\lambda f(t) + g(t))\mathrm{d}t = \frac{\lambda}{x}\int_0^x f(t)\mathrm{d}t + \frac{1}{x}\int_0^x g(t)\mathrm{d}t = \lambda T(f)(x) + T(g)(x)$$

On a de plus :

Ne pas oublier de vérifier l'égalité en 0

$$T(\lambda f + g)(0) = \lambda f(0) + g(0) = \lambda T(f)(0) + T(g)(0)$$

Ainsi :

$$\forall x \in \mathbb{R}_+,\ T(\lambda f + g)(x) = \lambda T(f)(x) + T(g)(x)$$

donc :

$$T(\lambda f + g) = \lambda T(f) + T(g)$$

T est donc un endomorphisme de E.

2. Raisonnons par analyse-synthèse.

Analyse. Soit $\lambda \in \mathbb{R}$ une valeur propre de T et f un vecteur propre associé. Pour tout réel $x > 0$, on a $T(f)(x) = \lambda f(x)$ donc en notant F l'unique primitive de f s'annulant en 0 :

$$\frac{F(x)}{x} = \lambda f(x)$$

Si $\lambda = 0$, on en déduit que F est nulle sur $\mathbb{R}_+^*$ donc $F' = f$ aussi. Par continuité en 0 on en déduit que f est la fonction nulle ce qui est impossible car f est un vecteur propre. Ainsi, $\lambda \neq 0$ et on a pour tout $x > 0$:

$$F(x) = \lambda x f(x) = \lambda x F'(x)$$

donc :

$$F'(x) = \frac{1}{\lambda x} F(x)$$

On reconnait alors une équation différentielle linéaire du premier ordre homogène dont le coefficient est une fonction continue. Il existe alors un réel C tel que :

$$\forall x > 0,\ F(x) = C\mathrm{e}^{\frac{\ln(x)}{\lambda}} = Cx^{\frac{1}{\lambda}}$$

Or $F' = f$ donc pour tout $x > 0$:

$$f(x) = Cx^{\frac{1-\lambda}{\lambda}}$$

Si $\frac{1-\lambda}{\lambda} < 0$ alors f admet une limite infinie (C est non nul car f est un vecteur propre) en 0 ce qui est impossible car f appartient à E. Ainsi,

$$\frac{1-\lambda}{\lambda} \geq 0$$

ce qui implique que $\lambda \in]0, 1]$. Remarquons que $T(f)(0) = \lambda f(0)$ donc $f(0) = \lambda f(0)$. Si $\lambda = 1$, alors f est constante sur $\mathbb{R}_+^*$ et continue sur $\mathbb{R}_+$ donc f est constante sur $\mathbb{R}_+$. Si λ est différent de 1 alors $f(0) = 0$ et on a bien :

$$\lim_{x \to 0} Cx^{\frac{1-\lambda}{\lambda}} = 0 = f(0)$$

car $\lambda \in]0, 1[$.

Synthèse. On vérifie facilement que tout réel $\lambda \in]0, 1]$ est valeur propre de T car :

$$f_\lambda : x \mapsto x^{\frac{1-\lambda}{\lambda}}$$

est une fonction non nulle de E et vérifiant $T(f_\lambda) = \lambda f_\lambda$. D'après l'analyse, on a de plus :

$$E_\lambda(T) \subset \mathrm{Vect}(f_\lambda)$$

ce qui nous donne finalement l'égalité :

$$E_\lambda(T) = \mathrm{Vect}(f_\lambda)$$

Tout autre réel n'est pas valeur propre de T d'après l'analyse.

3. 0 n'est pas valeur propre de T donc T est injective.

4. T n'est pas surjective car pour tout $f \in E$, $T(f)$ est dérivable sur $\mathbb{R}_+^*$ et il existe des fonctions de E non dérivables sur $\mathbb{R}_+^*$ ($x \mapsto |x - 1|$ par exemple).

Exercice 10 –

1. Vrai. On a :

$$A - 2\mathrm{I}_3 = \begin{pmatrix} -1 & 1 & 1 \\ 2 & -2 & 3 \\ 3 & -3 & 2 \end{pmatrix}$$

La matrice $A - 2\mathrm{I}_3$ n'est pas inversible car sa première colonne est l'opposée de la deuxième. On en déduit que 2 est valeur propre de A.

2. Faux. Le déterminant de A vaut 4 (qui est différent de 0) donc A est inversible et 0 n'est pas valeur propre de A.

3. Faux. La matrice A appartient à $\mathscr{M}_3(\mathbb{R})$ donc admet au maximum 3 valeurs propres réelles.

À retenir

- Une matrice de $\mathscr{M}_n(\mathbb{R})$ admet au plus n valeurs propres.
- Un endomorphisme d'un espace vectoriel de dimension n admet au plus n valeurs propres.